UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/863,384 | 05/24/2001 | Shingo Yamaguchi | 203223US-28 | 1503 |

22850 7590 08/09/2007

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| EXAMINER | |
|---|---|
| HA, LEYNNA A | |
| **ART UNIT** | **PAPER NUMBER** |
| 2135 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 08/09/2007 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application Number: 09/863,384
Filing Date: May 24, 2001
Appellant(s): YAMAGUCHI, SHINGO



James J. Kulbaski

For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 4/18/2007 appealing from the Office action mailed 1/23/2007.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

Claims 41-43, 45, 50-63, 65, and 70-80 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. patent 6,732,176 to Stewart et al. (herein "Stewart") and further in view of U.S. patent 6,453,159 to Lewis.

Claim 67 was cancelled in Amendment 1/20/2006, thus is not appealable.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

| | | |
|---|---|---|
| 6,732,176 | Stewart, et al. | 5-2004 |
| 6,453,159 | Lewis | 9-2002 |

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

*Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 41-43, 45, 50-63, 65, and 70-80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart, et al. (US 6,732,176) and in further view of Lewis (US 6,453,159).

As per claim 41:

Stewart, et al. discusses a method of controlling a network, comprising the steps of:

establishing a computer network connection between a computer and an intermediate device which has network resources connected thereto; (col.5, lines 2-14 and col.9, lines 30-35)

determining a level of security of the computer network connection based on determining whether the computer network connection to connect the computing device to the intermediate device (col.7, lines 46-61 and col.17, lines 10-15), wherein the first level of security is set and a second level of security is set; and (col.10, lines 20-24)

controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined (col.7, lines 35-59), such that the computing device is allowed access to a first set of network resources (col.13, lines 2-5 and col.15, lines 64-67), including a file server, based on a determined first level of security (col.16, lines 18-20 and 30-31), and is not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and email server, based on a determined second level of security (col.16, lines 21-29 and col.17, lines 28-32).

Stewart discloses setting and determining access levels according to the management information base (MIB) such that includes identification information and access information comprises access level or privilege level information (col.7, lines 24-45). The access level information is retrieved and used to determine a user's access to local network resources or Internet access (col.7, lines 55-61). Stewart teaches selectively allowing user access to different parts of the network (col.10, lines 20-24). Stewart teaches the second access level only allows external access such as the Internet (col.13, lines 18-31) where the visitor or customer that includes the access level to gain access to the Internet without being able to view any of the computing resources and file servers (col.16, lines 21-31. This reads on the claimed not allowed access to

the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and email server, based on a determined second level of security. Stewart reads on the first level of security where the access level or privilege level that have first access level information indicates which network resources on the local network (col.13, lines 2-6). As mentioned earlier, Stewart teaches that the second access level corresponds to access to the Internet and not the computing resources and file servers. Thus, it is obvious the second access level is allowed access to the computing resources and the file server is the claimed. Hence, Stewart reads on the claimed controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined, such that the computing device is allowed access to a first set of network resources, including a file server, based on a determined first level of security.

However, Stewart did not further discuss the computer network connection to connect the computing device to the intermediate device is encrypted, wherein the first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted.

Lewis teaches a wireless communication system that includes one or more mobile terminals (BMT) and access points connected the system backbone (col.4, lines 15-40) and more particularly to an encryption scheme for providing two or more levels of encryption to prevent unauthorized access to the network (col.1, lines 5-8). Lewis can

access the network without engaging in secure encrypted communications (col.5, lines 18-31) and providing levels of encryption in secure and non-secure format (col.5, lines 37-67). Lewis obviously discusses the secure access level as encrypted format that provides an ENCRYPT key to the access points and non-secure access level as non-encrypted format (col.9, lines 32-35 and col.13, lines 17-25). Lewis also includes a table which is a list of devices that are authorized to communicate with the network in either an encrypted or a non-encrypted format where encrypted is the first level of security and non-encrypted format is the claimed second level of security when the computer network connection is not encrypted (col.9, lines 61-64). Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart to include the computer network connection to connect the computing device to the intermediate device is encrypted, wherein the first level of security is set when it is determined that the computer network connection is encrypted as taught by Lewis because an encrypted connection is deemed authorized to communicate securely which prevents access to sensitive information and eavesdropping (col.5, lines 4-17). Further, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart to include a second level of security is set when it is determined that the computer network connection is not encrypted as taught by Lewis because non-encrypted connection is not secure and such non-encrypted manner is for communication link between the mobile terminal and the access point may initially be established (col.10, lines 60-63 and col.13, lines 17-25).

As per claim 42:See Stewart on COL.5, lines 15-19; discusses establishing a wireless computer network connection.

As per claim 43: See Stewart on COL.5, lines 20-21; discusses establishing a wireless computer network connection which conforms to an IEEE 802.11b standard

As per claim 44: Cancelled.

As per claim 45: See Lewis on COL.2, lines 14-24; discusses determining whether the computer network connection is encrypted using Wired Equivalent Privacy ("WEP") encryption

As per claims 46-49: Cancelled

As per claim 50: See Stewart on col.5, lines 5-8 and col.13, lines 44-55; discusses the step of determining is performed by the intermediate device, and said controlling is performed by the intermediate device.

As per claim 51: See Stewart on col.13, lines 44-55; discusses the step of determining is performed by the intermediate device which is a router.

As per claim 52: See Stewart on col.13, lines 44-55 and Lewis on col.15, lines 52-53; discusses the step of controlling is performed by the intermediate device which is a router having a firewall operation.

As per claim 53: See Stewart on col.5, lines 5-8 and col.13, lines 44-55; discusses the step of establishing is performed using the intermediate device which is a router which establishes a wireless connection to the computer.

As per claim 54: See Stewart on col.10, lines 2-3; discusses the step of determining is performed by a server running a network operating system, the server being different

from the intermediate device, and the step of controlling is performed by the server running the network operating system.

As per claim 55: See Stewart on COL.7, lines 30-42; discusses the step of determining is performed by the server which is running a network directory service.

As per claim 56: See Stewart on col.13, lines 44-55; discusses the step of establishing is performed by a bridge connected to the computer through the computer network connection.

As per claim 57: See Stewart on col.13, lines 44-55; discusses the step of establishing is performed by the bridge connected to the computer through the computer network connection which is a wireless network connection.

As per claim 58: See Stewart on col.9, lines 30-46 and Lewis on col.15, lines 52-53; discusses the level of access by a stand-alone firewall device which is connected between the intermediate device and the network resources.

As per claim 59: See Stewart on col.5, lines 44-54; discusses determining the level of security using the intermediate device.

As per claim 60: See Stewart on col.5, lines 5-8; establishing the computer network connection as a wireless connection using the intermediate device.

As per claim 61:

Stewart discloses a system for control a network that includes setting and determining access levels according to the management information base (MIB) such that includes identification information and access information comprises access level or privilege level information (col.7, lines 24-45). The access level information is retrieved

and used to determine a user's access to local network resources or Internet access (col.7, lines 55-61). Stewart teaches selectively allowing user access to different parts of the network (col.10, lines 20-24). Stewart teaches the second access level only allows external access such as the Internet (col.13, lines 18-31) where the visitor or customer that includes the access level to gain access to the Internet without being able to view any of the computing resources and file servers (col.16, lines 21-31. This reads on the claimed not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and email server, based on a determined second level of security. Stewart reads on the first level of security where the access level or privilege level that have first access level information indicates which network resources on the local network (col.13, lines 2-6). As mentioned earlier, Stewart teaches that the second access level corresponds to access to the Internet and not the computing resources and file servers. Thus, it is obvious the second access level is allowed access to the computing resources and the file server is the claimed. Hence, Stewart reads on the claimed controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined, such that the computing device is allowed access to a first set of network resources, including a file server, based on a determined first level of security.

However, Stewart did not further discuss the computer network connection to connect the computing device to the intermediate device is encrypted, wherein the first level of security is set when it is determined that the computer network connection is

encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted.

Lewis teaches a wireless communication system that includes one or more mobile terminals (BMT) and access points connected the system backbone (col.4, lines 15-40) and more particularly to an encryption scheme for providing two or more levels of encryption to prevent unauthorized access to the network (col.1, lines 5-8). Lewis can access the network without engaging in secure encrypted communications (col.5, lines 18-31) and providing levels of encryption in secure and non-secure format (col.5, lines 37-67). Lewis obviously discusses the secure access level as encrypted format that provides an ENCRYPT key to the access points and non-secure access level as non-encrypted format (col.9, lines 32-35 and col.13, lines 17-25). Lewis also includes a table which is a list of devices that are authorized to communicate with the network in either an encrypted or a non-encrypted format where encrypted is the first level of security and non-encrypted format is the claimed second level of security when the computer network connection is not encrypted (col.9, lines 61-64). Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart to include the computer network connection to connect the computing device to the intermediate device is encrypted, wherein the first level of security is set when it is determined that the computer network connection is encrypted as taught by Lewis because an encrypted connection is deemed authorized to communicate securely which prevents access to sensitive information and eavesdropping (col.5, lines 4-17). Further, it would have been obvious for a person of ordinary skills in the art to combine the

teaching of Stewart to include a second level of security is set when it is determined that the computer network connection is not encrypted as taught by Lewis because non-encrypted connection is not secure and such non-encrypted manner is for communication link between the mobile terminal and the access point may initially be established (col.10, lines 60-63 and col.13, lines 17-25).

As per claim 62: See Stewart on COL.5, lines 15-19; discusses establishing a wireless computer network connection.

As per claim 63: See Stewart on COL.5, lines 20-21; discusses establishing a wireless computer network connection which conforms to an IEEE 802.11b standard

As per claim 64: Cancelled.

As per claim 65: See Lewis on COL.2, lines 14-24; discusses determining whether the computer network connection is encrypted using Wired Equivalent Privacy ("WEP") encryption

As per claims 66-69: Cancelled.

As per claim 70: See Stewart on col.5, lines 5-8 and col.13, lines 44-55; discusses the means for determining is the intermediate device, and the means for controlling is the intermediate device.

As per claim 71: See Stewart on col.13, lines 44-55; discusses the means for determining is the intermediate device which is a router.

As per claim 72: See Stewart on col.13, lines 44-55 and Lewis on col.15, lines 52-53; discusses the means for controlling is the intermediate device which is a router having a firewall operation.

As per claim 73: See Stewart on col.5, lines 5-8 and col.13, lines 44-55; discusses the means for establishing is the intermediate device which is a router which establishes a wireless connection to the computer.

As per claim 74: See Stewart on col.10, lines 2-3; 24; discusses the means for determining is a server running a network operating system, the server being different from the intermediate device, and the means for controlling is the server running the network operating system.

As per claim 75: See Stewart on COL.7, lines 30-42; discusses the means for determining is the server which is running a network directory service.

As per claim 76: See Stewart on col.13, lines 44-55; discusses the means for establishing is a bridge connected to the computer through the computer network connection.

As per claim 77: See Stewart on col.13, lines 44-55; discusses the means for establishing is the bridge connected to the computer through the computer network connection which is a wireless network connection.

As per claim 78: See Stewart on col.9, lines 30-46 and Lewis on col.15, lines 52-53; discusses a stand-alone firewall device which is connected between the intermediate device and the network resources.

As per claim 79: See Stewart on col.5, lines 44-54; discusses means for determining the level of security using the intermediate device.

As per claim 80: See Stewart on col.5, lines 5-8; discusses means for establishing the computer network connection as a wireless connection using the intermediate device.

**(10) Response to Argument**

Examiner traverses the argument on page 7, that Stewart does not control a level of access to a network based on whether an encrypted or not-encrypted connection is made to the network.

Stewart teaches the network system includes one or more access points which communicate with a portable computing device 110 (PCD) in a wireless fashion (col.5, lines 3-8). The PCD 110 communicates with one of the access points 120 to gain access to network services such as the Internet access (col.5, lines 63-65). Stewart further discloses the access point and the PCD 110 are both equipped with an appropriate transmitter and receiver to establish a wireless communication link (col.6, lines 30-39). The claimed computer network connection can be reasonably interpreted as communicating or communication, wireless communication, communication link, or the act of communication access amongst devices of a network or between networks. Stewart discusses a management information base (MIB) that stores a data structure such as a table comprising a list of identification information, possible network providers, and access information. The access information comprises access level or privilege level information (col.7, lines 24-40). The PCD 110 begins communication with an access point where the network provider may be determined using this data

structure (col.7, lines 46-55) for selectively routing data between users and their corresponding network providers (col.8, lines 40-48). Stewart discloses the identification information also store access level information which may be used to indicate network access or privilege level and selectively allow user to different parts of the network (col.10, lines 20-24). Stewart further discusses the access point operates to direct PCD to an available communication channel based on the information received from the PCD where the access point assign channels for communication. The access point may also operate to direct the PCD 110 to an available communication channel based on other types of identification or authentication information, or on the determined access level of the PCD 110. This allows the access point to separate the communication traffic onto different channels based on the network provider being used or based on the access or privilege level of the PCD (col.14, lines 1-20). Thus, Stewart teaches the ability to access (different parts of) a communication network based on the access level information or privilege level. The access level information is reasonably considered as different levels of security of a connection. Stewart also discloses access level information may be used to determine a user's access to local network resources or Internet access which reads on the claimed controlling a level of access of the computing device to the network resources (col.7, lines 59-91).

Examiner traverses appellant's argument on page 8, that Lewis does not disclose or suggest setting a level of access to a network based on an encrypted or a not encrypted connection is made to the network. Lewis teaches an invention relates generally to wireless networks, and more particularly to an encryption scheme for

providing two or more levels of encryption to prevent unauthorized access to the network (col.1, lines 5-8). Similarly to Stewart, Lewis teaches a wireless communication system and a plurality of access points where each of the plurality of access points having a first transceiver for communicating wirelessly. The system includes a key distribution server configured to distribute a first encryption key to the plurality of mobile terminals where the encryption key is utilized to encrypt its wireless communications with the respective access point (col.2, lines 52-67). Appellant acknowledges (pg.8, 3rd paragraph) Lewis discloses a system device table 152 including a list of devices that can indicate devices authorized to communicate with the network in either encrypted or a non-encrypted format (col.9, lines 52-67). Further, the encrypted format is obviously secure to prevent from eavesdropping of sensitive information on wireless communications (col.5, lines 6-8 and col.10, lines 4-14), which is referring to the claimed first level of security when it is determined the computer network connection is encrypted. Whereas, non-encrypted format for non-sensitive information such that a communication link between the mobile terminal and the access point may initially be established (col.10, lines 15-27 and 60-63), which obviously is not secure. This is referring to the claimed second level of security is set when it is determined that the computer network connection is not encrypted.

Appellant stated that the claims are not directed to a system that pre-registers which access points are allowed to communicate in a non-encrypted or encrypted manner. However, claims 41 and 61 recite determining the level of security of whether the connection is encrypted or not encrypted. The claimed determining the level of

security does not include a method or device to carry out the process. Thus, using a table or a listing of data for determining the level of security (as in Lewis), a key or code to get the type/level of security, or by comparing pre-stored data with the device establishing connection is reasonably met the claimed determining the level of security. Lewis discloses an encryption key provided to access points in order to be used in communicating with the mobile terminals (col.9, lines 47-51). Lewis also discloses a system device table including a list of devices that can indicate devices authorized to communicate with the network in either encrypted or a non-encrypted format (col.9, lines 52-67). Lewis obviously suggests the use of the list of devices of the system device table to determine and to set the level of security. The list in Lewis represents a complete list of devices, which are authorized to communicate with the network (col.8, lines 31-41 and col.9, lines 61-63). Thus, the list of devices that are authorized to communicate with the network in either an encrypted and non-encrypted format suggests determining the computer communication network connection. This communication network connection is encrypted at different levels of security, such as a ($1^{st}$) level is set when it is determined that the computer network is encrypted and a ($2^{nd}$) level is set when it is determined the computer network connection is not encrypted (col.8, lines 31-41 and col.9, lines 47-67).

Examiner traverses the argument on page 10, where Lewis combined with the teachings in Stewart result in a system that allows access to different levels of a network based on pre-stored information about the different access elements which differs from the claims that recite determining a level of access based on whether an

encrypted or non-encrypted connection is made to the network. As discussed above, Stewart teaches having levels of access and security to the resources (col.12, lines 11-45 and col.13, lines 1-6) and connections (col.10, lines 20-24). Lewis teaches determining first and second levels of security of the computer network connection and setting the level of security as encrypted or non-encrypted format (col.9, lines 62-65). Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart with Lewis to teach pre-registered in the system device table for determining the levels of security of the computer network connection. The table lists the devices which are authorized to communicate with the network. Further, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart with Lewis to teach the first level of security for the computer network connection is set as encrypted and a second level of security set for the computer network connection is not encrypted. A connection set as encrypted is authorized to securely communicate and prevents access to sensitive information and eavesdropping (Lewis - col.5, lines 4-17). Thus, it is apparently obvious by setting a non-encrypted connection cannot securely communicate which would allow access to sensitive information and that the communication link between the mobile terminal and an access point may initially be established (Lewis - col.10, lines 60-63 and col.13, lines 17-25).

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Leynna Ha

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Kim Vu

Kambiz Zand

OBLON, SPIVAK, McCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314